



UNITED STATES PATENT AND TRADEMARK OFFICE

11
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,661	01/28/2002	James F. Riordan	CH9-2000-0011	8370
29683	7590	04/28/2006		EXAMINER
HARRINGTON & SMITH, LLP				CERVELLI, DAVID GARCIA
4 RESEARCH DRIVE				
SHELTON, CT 06484-6212			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 04/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	Application No.	Applicant(s)
	10/058,661	RIORDAN ET AL.
	Examiner	Art Unit
	David G. Cervetti	2136

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 07 April 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- The period for reply expires 3 months from the mailing date of the final rejection.
- The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because

- They raise new issues that would require further consideration and/or search (see NOTE below);
- They raise the issue of new matter (see NOTE below);
- They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
- They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. Applicant's reply has overcome the following rejection(s): _____.

6. Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. For purposes of appeal, the proposed amendment(s): a) will not be entered, or b) will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____

Claim(s) objected to: _____

Claim(s) rejected: 1-13

Claim(s) withdrawn from consideration: _____

AFFIDAVIT OR OTHER EVIDENCE

8. The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.

12. Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____

13. Other: _____

CHRISTOPHER REVAK
PRIMARY EXAMINER
Cll 4/26/08

Continuation of 11. does NOT place the application in condition for allowance because:

Chorley teaches publishing the public key, and the particular passage cited provides the teaching that publishing/knowledge of the encryption key, a plaintext and its corresponding encrypted text does not provide the decryption key.

Regarding Applicant's argument that Tschudin does not disclose or suggest ciphertext, etc, Examiner submits that Tschudin expressly teaches "apoptosis services"; encryption, decryption, or a key used for encryption/decryption, provide a service, and as such properly read on the claimed invention. The fact that Applicant chooses to use the term "apoptosis key" is not relevant, since an "apoptosis key" as disclosed does nothing more than provide a service, encryption or decryption, thus, the teachings provided by Tschudin and Kocher make a *prima fascie* case of obviousness.

An apoptosis key, as disclosed, is nothing more than a key that has been changed (dead, expired, not in use, etc). Thus, it would have been obvious to someone of ordinary skill in the art to check if an expired key is being used. Checking whether an expired key has been used to attempt access to a computer system is conventional and well known. Authentication methods for computer systems prompting users to change a password (key) after a certain amount of time had passed, were conventional and well known at the time the invention was made. It was also conventional and well known to prevent the re-use of a certain key by a certain user. This necessarily implies that an old key was saved to verify the user did not attempt to use the same key at a later time.

Furthermore, Tschudin expressly teach using a received key for decryption and looking at the result (test) to decide if it was a valid decryption or not (page 258), clearly contradicting Applicant's assertion that Kocher or Tschudin do not disclose or suggest "ciphertext", "test plaintext", "apoptosis key", etc. The decryption performed by Tschudin (page 258) clearly provides the teaching of using a key (apoptosis or not) and based on the result determining whether the decryption is valid or not. Tschudin clearly teaches checking using test values (page 258), namely "for each presented key we attempt to decrypt the ENCRYPTED_CODE. Looking at the result we can decide if this was a valid decryption or not."

Regarding Applicant's request for guidance, Examiner points Applicant to the following URL
<<http://www.uspto.gov/web/offices/com/sol/og/2005/week28/patbref.htm>> and the form needed PTO/SB/33 (Pre-Appeal Brief Request for Review).

DGC